State of Arizona

Department of Economic Security Information Technology Standards	Title: 1-38-0006 DES Information Security Policy	
Subject: Guidelines and responsibilities for the protection of State electronic information assets maintained by DES.	***Effective Date:*** 02/07/2000	***Revision:*** 1.3

1. Summary of Policy Changes

1.1. 02/07/02 – Results of an annual review. No substantive changes were implemented.

1.2. 10/15/03 – Major changes from DESS as a result of an annual review.

1.3. 10/29/04 – Minor changes to reflect the name change to the DTS Information Security Administration.

2. Purpose

This policy establishes guidelines and responsibilities for the protection of all State electronic information assets maintained by DES. Information and data are strategic assets and are used to conduct business for the State of Arizona. The purpose of information security is to ensure the integrity, confidentiality and availability of State owned information by preventing unauthorized access, modification or destruction.

2.1. Objectives

The primary objectives of this policy are to:

2.1.1. Prevent loss or misuse of DES information assets.

2.1.2. Maintain user accountability for protection of DES information assets.

2.1.3. Provide a secure framework that facilitates the sharing of information among State agencies and their partners.

3. Scope

This policy applies to all DES divisions and programs, boards, councils, and partners.

4. Responsibilities

4.1. The DES Director, Deputy Directors, Associate Directors, and Assistant Directors are responsible for enforcing this standard.

4.2 The Division of Technology Services (DTS) is responsible for providing initial and ongoing security related system identification, set-up and maintenance, based on policies, standards and other guidelines defined by DES Executive Management and the DES Security Authority. This responsibility extends to security related system software or hardware acquisition, settings or parameters within the DTS budgetary and physical control. DTS will provide ongoing technical consultation and recommendations concerning available security alternatives to permit appropriate security related policy, standard and guideline development.

4.3 The Information Security Administration (ISA) is the DES Security Authority and is responsible

for providing initial and ongoing security support for user set-up, maintenance, access provisioning, monitoring and incident response. This responsibility is currently fully implemented in the mainframe environment and will be extended to the network environment. The ISA also is responsible for participating in all security related policy, standard and guideline development and updating in both environments.

5. **Definitions and Abbreviations**

5.1. **Definitions**

5.1.1. **Information Assets -** In the context of this policy, information assets include the information technology infrastructure, applications, programs, databases and data elements that comprise them.

5.2. **Abbreviations and Acronyms**

5.2.1. **GITA** - **G**overnment **I**nformation **T**echnology **A**gency
5.2.2. **ARS** - **A**rizona **R**evised **S**tatutes
5.2.3. **DES –** **D**epartment of **E**conomic **S**ecurity
5.2.4. **DTS –** **D**ivision of **T**echnology **S**ervices
5.2.5. **ET –** DES **E**xecutive **T**eam
5.2.6. **IT –** **I**nformation **T**echnology
5.2.7. **ITSP** - **I**nformation **T**echnology **S**trategic **P**lan
5.2.8. **CIO** – **C**hief **I**nformation **O**fficer
5.2.9. **ISA –** **I**nformation **S**ecurity **A**dministration

6. **POLICY**

It is the policy of DES that:

6.1. Information assets under the stewardship of DES are strategic and vital resources belonging to the State of Arizona. These assets shall be available and protected commensurate with the value of the assets. Measures shall be taken to protect these assets against accidental or unauthorized access, disclosure, modification or destruction, as well as to assure the availability, integrity, utility, authenticity and confidentiality of information. Access to DES information assets shall be appropriately managed. A security training and awareness program shall be required for every user accessing DES data.

6.2. All DES systems and information shall remain the property of the DES. Consistent with this policy, none of the systems or information shall become the private property of any system user. Except as allowed under this policy, systems and information may be used only for the business of the State, as defined by the State, and shall reflect the image of the State.

6.3. The Director of DES is responsible for the protection of DES information assets~~.~~ To address this responsibility the Director authorized the creation of a Information Security Program. The Program, as detailed in the DES Information Security Guide, assigns operational responsibility for information/data custody and security. Division and Program Management are designated to serve as custodians, determining how information/data is created, maintained and protected. Security staffing, including Security Representatives, a Security Officer and a Security Planning Team (SPT) are also designated for implementing select security requirements; in consultation with Management.

6.4. All authorized users shall be accountable for their actions relating to information assets. Entering/altering/erasing DES data for direct or indirect personal gain or advantage, revealing DES data to persons who have not been specifically authorized to receive such data and attempting or achieving access to DES data not germane to mandated job duties are all actions prohibited and punishable under ARS 13-2316. Information assets shall be used only for intended purposes as defined by the agency and consistent with applicable laws

6.5. Risks to information assets shall be managed utilizing a formal risk assessment methodology designed to identify security vulnerabilities by type of exposure and probability of exposure. The expense of any resulting security safeguards shall be commensurate with the value of the assets being protected.

6.6. All authorized users of DES information systems or assets are responsible for following reasonable security measures and shall report any known or suspected security vulnerabilities or incidents to the appropriate management and security authority.

6.7. The integrity of data, its source, destination, and processes applied to it shall be assured. Changes to data shall be made only in authorized and acceptable ways.

6.8. Information assets shall be available when needed. Continuity of information assets critical to governmental services shall be ensured in the event of a disaster or business disruption. A disaster recovery plan shall be established, reviewed and tested to assure recovery and restoration of critical information assets.

6.9. Security requirements shall be identified, documented and addressed in all phases of development or acquisition of information assets.

6.10. Divisions shall ensure adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity.

6.11. Only State approved security tools shall be used on DES systems. A DES system shall not be used to attempt unauthorized access to any system or information.

6.12. The DES Director shall have responsibility for conducting an information asset inventory that is classified consistent with the Statewide Information Management Policy.

7. **Implications**

7.1. It is DES' responsibility to protect State information, to ensure information critical to DES services remains available in the event of disaster or business interruption, and to conduct an information asset inventory.

8. **Implementation Strategy**

8.1. All DES divisions and programs shall comply with this policy.

9. **References**

9.1. **Developmental References**

9.1.1. ARS, 41-3501 Definitions
9.1.2. ARS, 13-2316 Computer Tampering
9.1.3. DES Data Security Users Guide
9.1.4. DHHS Health Insurance Reform: Security Standards; Final Rule (HIPAA)

9.2. **Replaced References**

None

10. **Attachments**

None

11. **Associated GITA IT Standards or Policies**

11.1. P800 – IT Security Policy

11.2. S805 - Risk Management Standard

11.3. S810 - Account Management Standard

11.4. S815 – Configuration Management Standard

11.5. S820 – Authentication and Directory Services

11.6. S825 – Session Controls Standard

11.7. S830 – Network Security Standard

11.8. S850 – Encryption Technologies Standard

11.9. S855 - Incident Response and Reporting Standard

11.10. S860 – Virus and Malicious Code Protection Standard

11.11. S865 – Business Continuity/Disaster Recovery Plan (BCDR)

11.12. S870 – Backups Standard

11.13. S875 – Maintenance Standard

11.14. S880 – Media Sanitizing/Disposal Standard

11.15. S885 – Physical Security Standard

11.16. S890 - Personnel Security Standard

11.17. S895 – Security Training and Awareness Standard

12. **Review Date**

12.1. This document will be reviewed twelve (12) months from the original adoption date, and every twelve months thereafter.